Título del curso: Ciberseguridad y Amenazas a la Seguridad de los Estados.

Objetivo general:
Abordar los diferentes aspectos teóricos de la ciberguerra y de los conflictos armados digitales relacionados con la tecnología en el siglo XXI, dentro del marco de las relaciones internacionales y el derecho internacional público.

Objetivos específicos:
Comprender de manera integradora los diferentes aspectos teóricos de la ciberguerra y los conflictos armados contemporáneos en el marco de un contexto de interconexión e interdependencia. Conocer los diferentes actores, ámbitos y escenarios en los cuales se desarrolla la ciberguerra en la actualidad. Reflexionar sobre desafíos relativos a la ciberguerra y los conflictos armados contemporáneos en su relación con las relaciones internacionales y el derecho internacional público.

Dirigido a:
Profesionales que quieran profundizar sus conocimientos sobre las tensiones bélicas y su impacto en las dinámicas políticas, jurídicas, militares y económicas desarrolladas en el ciberespacio. Aspirantes y miembros de fuerzas armadas y cuerpos de seguridad, de las Fuerzas Armadas, del servicio diplomático y toda aquella persona que desarrolla actividades en el campo de las relaciones internacionales, el derecho, la seguridad informática y las ciencias sociales. Asimismo, profesionales, estudiantes o graduados interesados en ciberseguridad y su contexto global.

Al finalizar este curso los alumnos serán capaces de:

- Participar en instancias locales, regionales e internacionales donde se debaten los problemas actuales de la ciberguerra.
- Conocer los diferentes abordajes estratégicos en los conflictos armados digitales del siglo XXI. sus principales hitos y puntos de inflexión históricos.
- Aplicar un lenguaje específico orientado a las funciones tácticas y estratégicas relacionadas con la ciberguerra.
- Identificar infraestructuras críticas de la información y comprender los alcances de la interconexión creciente generada por la convergencia digital.
- Desarrollar capacidades analíticas de los diferentes abordajes de la temática.

MÓDULO 1: Aspectos generales de la ciberguerra y los conflictos digitales

Objetivos específicos:

1.a Comprender el fundamento, alcance e impacto de la ciberguerra y los conflictos digitales
1.b Conocer diferentes tipos de conflictos armados en el marco de internet
1.c Identificar los actores de la ciberguerra cibernética, sus roles y formas de interacción
1.d Reflexionar sobre las características específicas de los conflictos armados llevados a cabo mediante el uso de la tecnología.

Temario:

- Guerra en tiempos de internet
- Cuando el cibercrimen se convierte en conflicto armado
- Bloques regionales básicos
- ¿Qué tan seguros estamos en internet?

Referencias

- Foro Económico Global (2018). Informe de riesgos mundiales. Link: www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/the-global-risks-report-2018-es.pdf
- Castel, R. (2013). La inseguridad social. ¿Qué es estar protegido?. Buenos Aires, Editorial Manantial. Extracto del capítulo IV “Una nueva problemática del riesgo”.
- Stel, E. (2014). Seguridad y defensa del ciberespacio. Buenos Aires, Editorial Dunken. Extracto de la sección “Hechos ejemplificadores del ciberespacio”.

Preguntas abiertas

1. ¿Cómo se configura actualmente la geopolítica del poder militar en Internet?
2. ¿Cuál es el peor escenario que nuestro país podría enfrentar si se viera involucrado en una ciberguerra?

MÓDULO 2: Infraestructura de internet y su relación con la ciberguerra

Objetivos específicos:

2.a Aprender sobre los aspectos técnicos de internet vinculados con laciberguerra
2.b Identificar los diferentes tipos de infraestructura crítica
2.c Conocer los diferentes tipos de ataques relacionados con la infraestructura de internet

Temario:

- El campo de batalla de la ciberguerra
- La importancia de los puntos de conexión físicos
- Atacantes y atacados

Referencia

- Greenwald, G. (2014). Sin un lugar donde esconderse. Barcelona, Ediciones B. Extracto del capítulo III “Recogerlo todo”.

- Scolnik, H. (2014). Qué es la seguridad informática. Buenos Aires, Editorial Paidós. Extracto del capítulo I "¿Cuáles son los enemigos que acechan nuestro universo digital?".

Preguntas abiertas

1. ¿Qué tan material y físico es en realidad el espacio que consideramos digital e inmaterial?
2. En un escenario de ciberguerra, ¿Cuál es la principal infraestructura crítica que un atacante querría comprometer?

MÓDULO 3: Las relaciones internacionales y la ciberguerra

Objetivos específicos:

3.a Conocer los diferentes actores y ámbitos de discusión política relacionada con la ciberguerra
3.b Comprender las herramientas necesarias para las acciones diplomáticas en relación con la ciberguerra y evaluar su incidencia e impacto.
3.c Reflexionar sobre el rol de los Estados respecto de los derechos humanos en contexto de ciberguerra

Temario:

- Cuando la política se convierte en un arma informática
- La importancia de la e-diplomacia
- Los derechos humanos y el rol de los Estados en ciberguerra
- ¿Dónde se debate sobre la ciberguerra?

Referencias

- Ferrero, J. A. (2013). La ciberguerra. Génesis y evolución. Link: https://publicaciones.defensa.gob.es/media/downloadable/files/links/R/E/REVISTAS_PDF3296.pdf#page=82
- Cano, D. (2017). Jungla 3.0. Trolls, Información y desinformación. Buenos Aires, Pluma Digital Ediciones. Extracto del capítulo IV "Ataques y operaciones en el mundo de las redes sociales de segundo orden".

Preguntas abiertas

1. ¿Cómo debería reaccionar un gobierno interesado en protegerse contra las nuevas amenazas digitales a su soberanía?
2. ¿En qué espacios algunos gobiernos intentan construir consensos internacionales sobre ciberguerra?

MÓDULO 4: El derecho internacional público y la ciberguerra

Objetivos específicos:

4.a Conocer las normas internacionales aplicables en contexto de ciberguerra

4.b Entender la relación entre los diferentes actores intervinientes en los conflictos armados y su relación con el derecho internacional público
4.c Debatir sobre la incidencia de los actores privado en los conflictos armados tecnológicos

Temario:

- ¿Qué puede decir el derecho internacional sobre la ciberguerra?
- Cuando las empresas se convierten en participantes
- Protección de la ciudadanía

Referencia

- Sánchez, J. R. (2015) Artículo "Aspectos legales en el ciberespacio. La ciberguerra y el derecho internacional humanitario". Link: www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

Preguntas abiertas

1. ¿Por qué el derecho internacional público sigue vigente y es relevante para comprender el contexto internacional de la ciberguerra?
2. ¿Existe algún tratado de derecho internacional sobre ciberguerra?